BY ORDER OF THE COMMANDER
AIR FORCE MATERIEL COMMAND

AIR FORCE INSTRUCTION 14-303

AIR FORCE MATERIEL COMMAND
Supplement 1

30 DECEMBER 1999

Intelligence

RELEASE OF INTELLIGENCE TO US CONTRACTORS

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

NOTICE: This publication is available digitally on the HQ AFMC WWW site at: http://afmc.wpafb.af.mil. If you lack access, contact the Air Force Publishing Distribution Center (AFPDC).

OPR: HQ AFMC/INS (Terry Horseman)
Supersedes AFI14-303/AFMCS1, 6 Nov 96.

Certified by: HQ AFMC/INS (Col James A. Myers)
Pages: 12
Distribution: F

This supplement does not apply to the Air National Guard or US Air Force Reserve units and members.

SUMMARY OF REVISIONS

This supplement clearly defines responsibilities for the contract monitor and the designated center/tab research site Director of Intelligence (DI) and authorizes the DI to release intelligence data to AFMC contractors. It also establishes procedures for contractors requiring direct connectivity to SIPRNET. Specific guidance is also provided to ensure that the DD 254 clearly identifies that the contractor has intelligence requirements.

AFI 14-303, 1 Apr 99, is supplemented as follows:

1.2. The Director of Intelligence (HQ AFMC/IN) is the MAJCOM Senior Intelligence Officer (SIO). HQ AFMC/IN has designated each center/lab research site Director of Intelligence (DI) as the SIO for AFMC organizations. AFMC DI's are authorized to approve release of intelligence to AFMC contractors IAW AFI 14-303_AFMCSUP 1, provided there is a valid need-to-know and there is a current DD Form 254, **DoD Contract Security Classification Specification.** This authority does not include material labeled "Caution-Proprietary Information Involved" (PROPIN). Intelligence that bears the control marking "Dissemination and Extraction of Information Controlled By Originator" (abbreviated ORCON) may only be released to contractors within government facilities. Prior written permission from the originator of ORCON material must be obtained prior to its release to contractors outside government owned or controlled facilities.

1.2.1. US contractors requests for intelligence materials shall be submitted to the appropriate program manager according to local procedures and forwarded to the DI for release approval. This is usually worked through the contract monitor (CM). The AFMC Form 210, Intelligence Information Request, may be used for this purpose. In addition, the following guidance applies:

- No government official shall authorize the contractor use of intelligence materials on other contracts or release to subcontractors without express authority from the DI.
- The CM must specify on the DD Form 254 that disclosure does not create an unfair competitive advantage for the contractor, or a conflict of interest with the contractor's obligation to protect the information. If, during the course of the contract the contractor's requirements for information changes to require new or significantly different information, the DI or his/her designee shall make a new specification and certification. In cases where the designated official cannot or does not resolve the issue of unfair competitive advantage or conflict of interest, consent of the originator is required.
- Intelligence materials released under approved independent research and development (IR&D) efforts must be approved by the supporting DI and released to the sponsoring program manager.
- Intelligence materials may be provided at any phase of the contractual process or IR&D effort.
- If the release involves a contract from another command or service, but the CM resides within AFMC, the CM shall contact the local AFMC DI for releasability.
- The DI shall delete any reference to the Central Intelligence Agency, the phrase "Directorate of Operations" and any of its components, the place acquired, the field number, the source description, and field dissemination from all CIA Directorate of Operations reports passed to contractors, unless prior approval to do otherwise is obtained from the CIA.

1.2.2. (Added) Classified intelligence can be released to US contractors by the program office, or its designated field agency representative, provided prior approval has been obtained from the DI. Upon approval by the DI, a copy of the DD Form 254 and Visit Authorization will be on file in the DI's office before any discussions occur between a government official and a contractor.

1.2.3. (Added) Request for Information/Request for Proposal (RFP) Procedures. Selected intelligence materials may be approved for release by the supporting AFMC DI through the program manager to eligible contractors during any phase of the contracting process provided the sponsoring agency has determined that they have a valid need-to-know and there is a current DD Form 254.

1.2.4. (Added) Special Category Entities Contracted for Intelligence Support.

1.2.4.1. Federally Funded Research and Development Centers (FFRDC). Independent, private, not-for-profit corporations (unique entities) approved by the Secretary of the Air Force. FFRDCs support the United States Air Force (USAF) and operate under government procedures and constraints appropriate to their noncompetitive mission. Specific FFRDC elements have been designated to conduct threat related analyses as integral parts of US government offices.

1.2.4.2. Government Owned-Contractor Operated (GOCO) Activities. GOCOs may handle and control intelligence in the same manner as US government offices. GOCO activities are not considered contractors if they perform classified services in support of the intelligence mission of an organization. They should be designated as such by the HQ USAF/XOI, or other department/agency senior officials of the intelligence communities.

1.2.4.3. Service and Manpower Support Contrators. Contractors who perform system engineering and technical assistance in direct support to AFMC program offices. Program offices acquire their services to increase the design performance capabilities of existing, new, or emerging systems. Their services are integral to the logistics support and maintenance of a system or major component, or end item of equipment essential to the operation of the system before final government acceptance of a complete hardware

system. They are barred from negotiating for manufacturing work on contracts for which they are providing support.

1.2.4.4. Special Purpose Agreement (not a contract). The Intergovernmental Personnel Act (IPA) of 1970 provides for the temporary detail of employees from state and local governments, Indian tribal governments, institutions of higher education, qualifying nonprofit organizations, etc., to an agency of the Federal Government.

1.2.5. (Added) Release of Intelligence for IR&D Efforts. IR&D efforts are IR&D efforts initiated, conducted, and funded by companies which fall within the four following areas:

- Basic research.
- Applied research.
- Development.
- Systems and other concept formulation studies.

A Memorandum of Understanding (MOU) is required for release of intelligence materials. The MOU must be signed by the commander or director of the sponsoring organization who has primary interest in tracking the proposed IR&D project and any intelligence data released under an MOU must be approved by the supporting AFMC DI.

1.2.5.1. The DI will send a copy of the MOU to HQ AFMC/IN and maintain a listing of intelligence materials released. The government sponsor is responsible for the return of all released intelligence materials after completion of the IR&D effort and no later than the end of the MOU term. This must be accomplished within 30 calendar days after the completion or termination of the company's IR&D project.

1.2.5.2. The MOU may be extended for another term. The following will be added to the extension: "Attached agreement is in full force and effective from _____ to _____." The government sponsor will sign the MOU extension below this statement and provide a copy to the DI. The DI will ensure AFMC/IN receives a copy of the MOU extension.

1.2.6. (Added) For contracts, the CM shall:

- Ensure the DD Form 254 (block 10e) clearly identifies that the contractor has intelligence requirements. The DD Form 254 provides the contractor with security requirements and classification guidance and is coordinated with the local Industrial Security Office. When block 10e is marked "YES," this denotes the fact that intelligence data will be required. The CM is then responsible for contacting the local AFMC DI to review and coordinate on the package. Also, ensure block 13. Security Guidance, has the following statement: "Contractor will require access to and must comply with AFI 14-303 and AFMC Supplement 1."
- Maintain a record of all intelligence materials released to the contractor, and furnish the DI with a listing upon the DI's request.
- Contractors must return intelligence data to the CM at termination or completion of a contract. On a case-by-case basis, requests for retention of intelligence material by the contractor past expiration date of contract must be submitted in writing to the CM for approval by the DI.
- Intelligence holdings can be transferred to another contract within the same company provided the DD Form 254 requirements are met and approved by the CM.

1.2.7. (Added) Special Requirements for General Intelligence Material. In addition to AFI 14-303 and AFMC Supt 1, the Director of Central Intelligence, sets up additional requirements and controls for intelligence in the possession of contractors. The contractor shall:

- Understand that intelligence released to contractors, all reproductions thereof, and all other material generated based on, or incorporating data therefrom (including authorized reproductions), remain the property of the US government.
- Understand all reproductions and extractions of intelligence shall be classified, marked, and controlled in the same manner as the original(s).
- Not further disclose or release intelligence to any of their components or employees, or to another contractor (including subcontractors), without the prior written notification and approval of the SOIC, or his/her designee, unless such disclosure or release is authorized in writing at the initiation of the contract as an operational requirement. (Refer toAFI14-303_ AFMCSUP 1, paragraph 1.2 for further guidance.)
- Ensure that each employee having access to intelligence material complies with AFI 14-303 and AFMC Supplement 1.

1.3.1. (Added) National Intelligence Estimates (NIE), Special National Intelligence Estimates (SNIE), and Interagency Intelligence Memoranda may be released to appropriately cleared contractors possessing an appropriate level facility clearance and need-to-know, except as regulated by provisions concerning proprietary information. Requests shall be submitted to HQ AFMC/IN through the local DI for release approval.

6. (Added) Access to intelligence information via electronic connectivity (SIPRNET/INTELINK-S), or within another government office, must be submitted in writing to the CM for approval by the DI (IAW HQ AFMC Policy) (attachment 1(Added)). Access to intelligence data via electronic connectivity is a separate process from the DD Form 254, but will be incorporated into the DD Form 254 upon final approval.

7. (Added) Release of Classified and Unclassified Information to Foreign Owned Companies and Their Representatives. Any military activity or defense contractor receiving a request from a foreign owned company, or a representative thereof, for intelligence data about this program, shall forward the request to the servicing Foreign Disclosure Policy Office.

Attachment 1

(ADDED) GLOSSARY OF ABBREVIATIONS, ACRONYMS, AND TERMS

Abbreviations and Acronyms

CM—Contract Monitor

DI—Director of Intellligence

DISA—Defense Information Systems Agency

DISN—Defense Information Systems Network

FFRDC—Federally-Funded Research and Development Center

GOCO— Government Owned-Contractor Operated

IR&D— Independent Research & Development

IPA—Intergovernmental Personnel Act

MOU—Memorandum of Understanding

RFP—Request for Proposal

Terms

AFMC Form 210— Intelligence Information Request.

Contract Monitor— The representative of a project office responsible for the technical/administrative management of contract performance and who establishes the security requirements applicable to the contract. The CM provides guidance and assistance (through appropriate command channels) as necessary for the procuring contracting officer and the administrative contracting officer to exercise their responsibilities.

Contracting Officer— A person with authority to enter into, administer, and/or terminate contracts and make related determinations and findings.

DD Form 254—Contract Security Classification Specification.

Director of Intelligence (DI)— The DI is the center/lab research site Senior Intelligence Officer (SIO). The DI is responsible for the planning and execution of intelligence functions supporting all AFMC intelligence requirements; as the SIO, serves as the intelligence staff officer for the commander/director of each center/lab research site.

Independent Research and Development (IR&D)— A contractor's research and development project falling within the four following areas:

Memorandum of Understanding (MOU)— A written agreement between a company and a USAF organization describing specific classified projects or technology areas which will require intelligence data support. The MOU will be effective for 2 years but may be renewed.

National Industrial Security Program Operating Manual— Prescribes requirements, restrictions, and other safeguards necessary to prevent unauthorized disclosure of classified information and to control authorized disclosure of classified information released by US government executive branch departments

and agencies to their contractors.

Releasing Agent— CM of contracting activity.

Sponsoring Organization— The government organization interested in a company IR&D project.

Attachment 2
CONTRACTOR ACCESS TO SECRET INTERNET PROTOCOL ROUTABLE NETWORK (SIPRNET) AND INTELINK-S

A2.1. CONTRACTOR CONNECTIVITY TO SIPRNET IN CONTRACTOR-CONTROLLED FACILITIES OFF BASE: SIPRNET is a Secret US Only system. All CONUS off-base contractor customers desiring a direct connection to the SIPRNET must comply with the following procedures:

A2.1.1 Contractor will consult with the Contract Monitor (CM) and local Director of Intelligence (DI) regarding the feasibility of the connectivity.

A2.1.2. Contractor will contact Defense Information Systems Agency (DISA) Project Manager and request a Systems Security Package for completion.

A2.1.3. The package will be completed by the contractor and forwarded to the Contract Monitor.

A2.1.4.The CM will verify the contractors need for connection to SIPRNET, coordinate with local DI (see #1.b., CONTRACTOR ACCESS TO INTELINK-S below), sign and forward the package to DISA. Regardless of whether the contractor desires access to intelligence via SIPRNET, coordination with the local DI will be accomplished and incorporated into the package to be submitted to DISA.

A2.1.5. DISA reviews the Systems Security Package; verifies through Defense Security Service (DSS) that the contractor has a valid contractor facility clearance; requests DSS to conduct a Site Inspection for a dedicated connection to SIPRNET; obtains validation by Joint Staff/J6T.

A2.2. CONTRACTOR ACCESS TO INTELINK-S OFF BASE IN CONTRACTOR-CONTROLLED FACILITIES:

A2.2.1. The CM must submit the request for access to specific intelligence obtainable through INTELINK-S. The local DI will assist in identifying the intelligence needed in support of the contract (i.e., what web sites the contractor should be allowed access to). The CM will obtain from the local DI approval in writing. The CM must comply with DCID 1/7 and AFI 14-303 with AFMC Supplement 1. The local DI will coordinate with any outside agencies as required for proper release of intelligence. The contractor will only have access to intelligence information needed to fulfill specific contractor obligations IAW with their existing contracts.

A2.2.2. DISA and the Defense Information Systems Network (DISN) Air Force Action Officer is supplied the above information by the CM with the local DI's approval in writing.

A2.2.3. Firewalls/PROXY SERVERS will be installed on that system by DISA to prevent the contractor from accessing other intelligence information not related to the contract.

A2.3. CONTRACTOR CONNECTIVITY TO SIPRNET IN CONTRACTOR-CONTROLLED FACILITIES ON BASE : SIPRNET is a Secret US Only system. All CONUS on-base contractor customers desiring a direct connection to the SIPRNET must comply with the following procedures:

A2.3.1. Contractor will consult with the Contract Monitor (CM) and local DI regarding the feasibility of the connectivity.

A2.3.2. The CM will verify the contractors need for connection to SIPRNET and coordinate with local DI (see #2.b., CONTRACTOR ACCESS TO INTELINK-S, below). Regardless of whether the contractor desires access to intelligence via SIPRNET, coordination with the local DI will be accomplished and

incorporated into the package to be submitted to the Communications Group.

A2.3.3. The CM will contact the local Communications Group office for directions on the correct paperwork to submit for SIPRNET connectivity.

A2.4. CONTRACTOR ACCESS TO INTELINK-S ON BASE IN CONTRACTOR-CONTROLLED FACILITIES: The CM must submit the request for access to specific intelligence obtainable through INTELINK-S. The local DI will assist in identifying the intelligence needed in support of the contract (i.e., what web sites the contractor should be allowed access to). The CM will obtain from the local DI approval in writing. The CM must comply with DCID 1/7 and AFI 14-303 with AFMC Supplement 1. The local DI will coordinate with any outside agencies as required for proper release of intelligence. The contractor will only have access to intelligence information needed to fulfill specific contractor obligations in accordance with their existing contracts.

A2.5. AFMC POLICY ON COLLATERAL CONTRACTOR ACCESS TO INTELINK-S WITHIN GOVERNMENT FACILITIES:

A2.5.1. Contractors clearance at the SECRET level or higher and DD Form 254 will be on file in the government facility allowing access to INTELINK-S.

A2.5.2. The Contractor's DD Form 254 must have blocks 10b, d, e(2), h and j marked "Yes."

A2.5.3. If the government facility IS NOT the local intelligence office, then a letter will be submitted by the CM to the local DI requesting approval for their contractor(s) to have access to INTELINK-S. The letter will include the following information: Contractor's Last Name, First Name, MI, Social Security Number, Duty Phone, Program, Government Organizational Office Symbol, Government Organizational Address, Position Description/Job Title, Building/Room Number, E-mail address. The local DI will make every effort to assist the CM in the proper procedures for their contractor's to have access to INTELINK-S.

A2.5.4. Contractor must certify in writing (sign/date):

A2.5.1.1. The computer account will be used in support of an official government project.

A2.5.1.2. I will not willfully compromise the account password.

A2.5.1.3. I will notify the CM when the account is no longer needed, account information needs revising, or the account password has been knowingly compromised.

A2.5.1.4. The account will be used in accordance with all existing instructions, policy directives and guidelines to ensure no improper or fraudulent use.

A2.5.1.5. Data and files associated with this account are subject to random review.

A2.5.1.6. The account password will be changed in accordance with current Air Force policy.

A2.5.17. I am responsible for not only safeguarding the classified contents of this account, but also the physical configuration of the network.

A2.5.1.8. Access to intelligence information does not include PROPIN.

Attachment 3
CONTRACTOR ACCESS TO SECRET INTERNET PROTOCOL ROUTABLE NETWORK (SIPRNET) AND INTELINK-S

DEPARTMENT OF DEFENSE
CONTRACT SECURITY CLASSIFICATION SPECIFICATION

(The requirements of the DoD Industrial Security Manual apply to all security aspects of this effort)

1. CLEARANCE AND SAFEGUARDING
a. FACILITY CLEARANCE REQUIRED
b. LEVEL OF SAFEGUARDING REQUIRED

2. THIS SPECIFICATION IS FOR: *(X and complete as applicable)*
- a. PRIME CONTRACT NUMBER
- b. SUBCONTRACT NUMBER
- c SOLICITATION OR OTHER NUMBER — DUE Date *(YYMMDD)*

3. THIS SPECIFICATION IS: *(X and complete as applicable)*
- a. ORIGINAL *(Complete date in all cases)* — Date *(YYMMDD)*
- b. REVISED *(Supersedes all previous specs)* — Revision No. — Date *(YYMMDD)*
- c. FINAL *(Complete Item 5 in all cases)* — Date *(YYMMDD)*

4. IS THIS A FOLLOW-ON CONTRACT? ☐ YES ☐ NO. If Yes, complete the following:
Classified material received or generated under _____ *(Preceding Contract Number)* is transferred to this follow-on contract

5. IS THIS A FINAL DD FORM 254? ☐ YES ☐ NO. If Yes, complete the following:
In response to the contractor's requested dated _____, retention of the identified classified material is authorized for the period of _____

6. CONTRACTOR *(Include Commercial and Government Entity (CAGE) Code)*

a. NAME, ADDRESS, AND ZIP CODE	b. CAGE CODE	c. COGNIZANT SECURITY OFFICE *(Name, Address, and Zip Code)*

7. SUBCONTRACTOR

a. NAME, ADDRESS, AND ZIP CODE	b. CAGE CODE	c. COGNIZANT SECURITY OFFICE *(Name, Address, and Zip Code)*

8. ACTUAL PERFORMANCE

a. LOCATION	b. CAGE CODE	c. COGNIZANT SECURITY OFFICE *(Name, Address, and Zip Code)*

9. GENERAL IDENTIFICATION OF THIS PROCUREMENT

10. THIS CONTRACT WILL REQUIRE ACCESS TO:	YES	NO	11. IN PERFORMING THIS CONTRACT, THE CONTRACTOR WILL:	YES	NO
a. COMMUNICATIONS SECURITY (COMSEC) INFORMATION			a. HAVE ACCESS TO CLASSIFIED INFORMATION ONLY AT ANOTHER CONTRACTOR'S FACILITY OR A GOVERNMENT ACTIVITY		
b. RESTRICTED DATA			b. RECEIVE CLASSIFIED DOCUMENTS ONLY		
c. CRITICAL NUCLEAR WEAPON DESIGN INFORMATION			c. RECEIVE AND GENERATE CLASSIFIED MATERIAL		
d. FORMERLY RESTRICTED DATA			d. FABRICATE, MODIFY, OR STORE CLASSIFIED HARDWARE		
e. INTELLIGENCE INFORMATION			e. PERFORM SERVICES ONLY		
(1) Sensitive Compartmented Information (SCI)			f. HAVE ACCESS TO U.S. CLASSIFIED INFORMATION OUTSIDE THE U.S. PUERTO RICO, U.S. POSSESSIONS AND TRUST TERRITORIES		
(2) Non-SCI			g. BE AUTHORIZED TO USE THE SERVICES OF DEFENSE TECHNICAL INFORMATION CENTER (DTIC) OR OTHER SECONDARY DISTRIBUTION CENTER		
f. SPECIAL ACCESS INFORMATION			h. REQUIRE A COMSEC ACCOUNT		
g. NATO INFORMATION			i. HAVE TEMPEST REQUIREMENTS		
h. FOREIGN GOVERNMENT INFORMATION			j. HAVE OPERATIONS SECURITY (OPSEC) REQUIREMENTS		
i. LIMITED DISSEMINATION INFORMATION			k. BE AUTHORIZED TO USE THE DEFENSE COURIER SERVICE		
j. FOR OFFICIAL USE ONLY INFORMATION			l. OTHER *(Specify)*		
k. OTHER *(Specify)*					

DD Form 254, DEC 90 ***(EF-V1)*** *(PerFORM PRO)* *Previous editions are obsolete.*

12. PUBLIC RELEASE. Any information (classified or unclassified) pertaining to this contract shall not be released for public dissemination except as provided by the Industrial Security Manual or unless it has been approved for public release by appropriate Government authority. Proposed public releases shall be submitted for approval prior to release

[ ] Direct [ ] Through *(Specify):*

to the Directorate for Freedom of Information and Security Review, Office of the Assistant Secretary of Defense (Public Affairs) for review.
In the case of non-DoD User Agencies, requests for disclosure shall be submitted to that agency.

13. SECURITY GUIDANCE. The security classification guidance need for this classified effort is identified below. If any difficulty is encountered in applying this guidance or if any other contributing factor indicates a need for changes in this guidance, the contractor is authorized and encouraged to provide recommended changes; to challenge the guidance or the classification assigned to any information or material furnished or generated under this contract; and to submit any questions for interpretation of this guidance to the official identified below. Pending final decision, the information involved shall be handled and protected at the highest level of classification assigned or recommended. *(Fill in as appropriate for the classified effort. Attach, or forward under separate correspondence, any document/guidelines/extracts reference herein. Add additional pages as needed to provide complete guidance.)*

14. ADDITIONAL SECURITY REQUIREMENTS. Requirements, in addition to ISM requirements, are established for this contract. *(If Yes, identify the pertinent contractual clauses in the contract document itself, or provide an appropriate statement which identifies the additional requirements. Provide a copy of the requirements to the cognizant security office. Use Item 13 if additional space is needed)* [ ] Yes [ ] No

15. INSPECTIONS. Elements of this contract are outside the inspection responsibility of the cognizant security office. *(If Yes, identify specific areas or elements carved out and the activity responsible for inspections. Use Item 13 if additional space is needed.)* [ ] Yes [ ] No

16. CERTIFICATION AND SIGNATURE. Security requirements stated herein are complete and adequate for safeguarding the classified information to be released or generated under this classified effort. All questions shall be referred to the official named below.

a. TYPED NAME OF CERTIFYING OFFICIAL	b. TITLE	c. TELEPHONE *(Include Area Code)*
d. ADDRESS *(Include Zip Code)*		
e. SIGNATURE		

17. REQUIRED DISTRIBUTION

- [ ] a. CONTRACTOR
- [ ] b. SUBCONTRACTOR
- [ ] c. COGNIZANT SECURITY OFFICE FOR PRIME AND SUBCONTRACTOR
- [ ] d. U.S. ACTIVITY RESPONSIBLE FOR OVERSEAS SECURITY ADMINISTRATION
- [ ] e. ADMINISTRATION CONTRACTING OFFICER
- [ ] f. OTHERS AS NECESSARY

DD Form 254, DEC 90 *(REVERSE) (EF-V1) (PerFORM PRO)*

STEWART E. CRANSTON, Lt. Gen., USAF
Vice Commander